UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,344	08/16/2001	Massimiliano Antonio Poletto	12221-004001	2635

26161 7590 04/19/2006

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,344	POLETTO ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/16/1 & 3/4/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-39 have been re-examined and are pending.

2. This is a Final rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Yavatkar, et al. (US 6,735,702).

As per claim 1:

discloses gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises: a computing device comprising:

a monitoring process that monitors network traffic through the gateway;

[col.1, lines and col.7, lines 43-48]

a communication process that communicate statistics collected **[col.2, lines 4-5 and 53-60 and col.3, lines 28-45; statistics from the monitoring process is inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway.]** in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center; **[col.3, lines 25-29 and col.11, lines 51-55]**

and a filtering process to insert filters on network devices **[col.3, lines 46-53 and col.13, lines 56-62]** to filter out packets that the gateway deems to be part of an attack. **[col.20, lines 20-21]**

As per claim 2: See col.2, lines 57-59; discussing the communication process couples to a dedicated link to communicate with the control center over a hardened network.

As per claim 3: See col.7, lines 43-45; discussing the monitoring process in the gateway samples network packet flow in the network.

As per claim 4: See col.7, lines 43-44; discussing the gateway is adaptable to be physically deployed in line in the network.

As per claim 5: See col.14, lines 26-28 and col.15, lines 38-39; discussing the gateway is adaptable to dynamically install filters on nearby routers.

As per claim 6: See col.13, lines 4-29 and col.15, lines 30-33; discussing the monitoring process detects IP traffic and determines levels of unusual

amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

As per claim 7: See col.13, lines 44-53 and col.15, lines 19-21; discussing the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

As per claim 8: See col.13, lines 4-29 and col.15, lines 30-33; discussing monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports.

As per claim 9: See col.15, lines 30-33; discussing monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

As per claim 10: See col.1, lines 27-31; discussing monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection.

As per claim 11: See col.2, lines 53-55; discussing monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail.

As per claim 12: See col.2, lines 4-5 and col.3, lines 30-32; discussing monitoring process maintains statistics on parameters including source and

destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

As per claim 13: See col.14, lines 54-58 and col.15, lines 26-27; discussing monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold.

As per claim 14: See col.2, lines 4-5; discussing monitoring process logs packets.

As per claim 15: See col.5, lines 13-20 and col.13, lines 61-63; discussing monitoring process logs specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

As per claim 16:

method of protecting a victim site during a denial of service attack, comprises:

disposing a gateway device between the victim site and a network; **[col.7, lines 43-48]**

monitoring network traffic through the gateway and measuring heuristics of the network traffic to provide statistics network traffic; **[col.2, lines 4-5 and 53-60 and col.3, lines 28-45; statistics from the monitoring process is inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway.]**

communicating the statistics collected in the gateway to a control center; **[col.10, lines 15-17 and col.14, lines 59-65]**

and filtering out packets that the gateway or control center deems to be part of an attack. **[col.13, lines 53-62 and col.20, lines 20-21]**

As per claim 17: **See col.2, lines 57-59;** discussing communicating occurs over a dedicated link to the control center via a hardened network.

As per claim 18: **See col.2, lines 53-55 and col.7, lines 43-45;** discussing monitoring samples network packet flow in the network.

As per claim 19: **See col.7, lines 43-44;** discussing the gateway is physically deployed in line in the network.

As per claim 20: **See col.14, lines 26-28 and col.15, lines 38-39;** discussing filtering further comprises: dynamically installing filters on nearby routers via an out of band connection.

As per claim 21: **See col.13, lines 4-29 and col.15, lines 30-33;** discussing monitoring further comprises: detecting IP traffic and determining levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

As per claim 22: **See col.13, lines 44-53 and col.15, lines 19-21;** discussing monitoring further comprises: detecting Internet Protocol (IP) traffic and determining levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

As per claim 23: **See col.13, lines 4-29 and col.15, lines 30-33;**

discussing monitoring further comprises: detecting Internet Protocol (IP) traffic and determining levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

As per claim 24: **See col.15, lines 30-33;** discussing monitoring further comprises: detecting IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

As per claim 25: **See col.1, lines 27-31;** discussing monitoring further comprises: detecting a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

As per claim 26: **See col.2, lines 4-5 and col.3, lines 30-32;** discussing monitoring further comprises: logging statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

As per claim 27: **See col.14, lines 54-58 and col.15, lines 26-27;** discussing monitoring further comprises: issuing a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

As per claim 28: **See col.5, lines 13-20 and col.13, lines 61-63;** discussing monitoring further comprises: logging specific packets identified as part of an attack to enable an administrator to identify important properties of

the attack.

As per claim 29:

computer program product residing on a computer readable medium for protecting a victim site during a denial of service attack, comprises instructions for causing a computer device coupled at an entry to the site to:

monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic; **[col.2, lines 4-5 and 53-60 and col.3, lines 28-45; statistics from the monitoring process is inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway.]**

communicate statistics collected in the computer device to a control center; and **[col.2, lines 4-5 and col.3, lines 30-38]**

filter out packets that the device or control center deems to be part of an attack. **[col.13, lines 53-62 and col.20, lines 20-21]**

As per claim 30: **See col.2, lines 53-55;** discussing sample network traffic flow.

As per claim 31: **See col.14, lines 26-28 and col.15, lines 38-39;** discussing instructions to filter further comprise instructions to: dynamically install filters on nearby routers via an out of band connection.

As per claim 32: **See col.13, lines 4-29 and col.15, lines 30-33;** discussing instructions to monitor further comprise instructions to: detect IP traffic; and determine levels of unusual amounts of IP fragmentation or

fragmented IP packets with bad or overlapping fragment offsets.

As per claim 33: **See col.13, lines 44-53 and col.15, lines 19-21;** discussing instructions to monitor further comprise instructions to: detect Internet Protocol (IP) traffic; and determine levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

As per claim 34: **See col.13, lines 4-29 and col.15, lines 30-33;** discussing instructions to monitor further comprise instructions to: detect Internet Protocol (IP) traffic; and determine levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

As per claim 35: **See col.15, lines 30-33;** discussing instructions to monitor further comprises instructions to: detect IP traffic; and determine levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

As per claim 36: **See col.1, lines 27-31;** discussing instructions to monitor further comprises instructions to: detect a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

As per claim 37: **See col.2, lines 4-5 and col.3, lines 30-32;** discussing instructions to monitor further comprises instructions to: log statistics on parameters including source and destination host or network

addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

As per claim 38: **See col.14, lines 54-58 and col.15, lines 26-27;** discussing instructions to monitor further comprises instructions to: issue a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

As per claim 39: **See col.7, lines 43-55;** discussing instructions to cause the processor to receive communications from a control center to deliver data pertaining to the types of traffic passing through the gateway.

Response to Arguments

4. Applicant's arguments with respect to claims 1-39 have been considered but are not persuasive.

The claimed invention broadly claims to insert filters on network devices where this can be any device that is within or on a network. Hence, the network device is in the form of network nodes or a gateway where the filters are positioned or inserted at the network nodes (col.3, lines 48-50 and col.7, lines 43-48). Statistics was not limited to any kind or what is involved as part of the statistic in applicant's invention. Statistics from the monitoring process is inherently gathered data of similarities or differences used for analysis purposes where the gathered data from the monitoring process is to determine

the attacks and kind of traffic on the gateway (col.2, lines 4-5 and 53-60 and col.3, lines 28-45).

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone

number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KAMBIZ ZAND
PRIMARY EXAMINER

LHa